Міністерство освіти і науки України Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

«Криптографія»

Лабораторна робота №2

«Кпиптофналіз шифру Віженера»

Виконав

студент групи ФБ-93

Флекевчук Данило

Київ – 2021

Мета: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі:

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Частина 1

Для виявлення залежностей в методах дослідження тексту було обрано фрагменти з твору «Злочин і кара» Ф.М Достоєвського. Я шифрував текст алгоритмом за алгоритмом шифру Віженера для ключів довжиною 2-5 та 10-20 символів. Далі для першої групи ШТ(2-5) я проводив аналіз на індекс відповідності, для другого рахував через символ Кронекера.

Для Прешого методу статистика.

Методом Індексів			
key= рв len= 2	key= узс len= 3	key= зслу len= 4	key= вшувз len= 5
2 0.057472049440222	2 0.03787409051999	2 0.045588705354506	2 0.03659494016428
3 0.044368980937942	3 0.05740200664733	3 0.036952088776427	3 0.03653994851250
4 0.057477648871460	4 0.03784780618135	4 0.057477648871460	4 0.03664628799436
5 0.044355027305547	5 0.03779472209912	5 0.036965436356927	5 0.05739750264722

Провівши аналіз ми бачимо що при правильній довжині ключа ми бачимо, що індекс прямує до індексу визначеного для російської мови. Також ми бачимо для кратних довжин йде кореляція результатів. Це повязано з методом обрахунку індексу саме з поділом на блоки.

Для Другого методу.

Методом	Символів	Кронекера		
key=флфлцхювге len= 10	key=аопретиоенк len= 11	key=аопренлскгек len= 12	key= аопренлскгеки len= 13	key=аопренксокекик len= 14
732 - key length= 10	398 - key length= 10	436 - key length= 10	449 - key length= 10	475 - key length= 10
453 - key length= 11	823 - key length= 11	437 - key length= 11	404 - key length= 11	449 - key length= 11
454 - key length= 12	395 - key length= 12	742 - key length= 12	395 - key length= 12	487 - key length= 12
353 - key length= 13	465 - key length= 13	379 - key length= 13	792 - key length= 13	448 - key length= 13
378 - key length= 14	464 - key length= 14	468 - key length= 14	380 - key length= 14	782 - key length= 14
345 - key length= 15	450 - key length= 15	478 - key length= 15	464 - key length= 15	462 - key length= 15
373 - key length= 16	452 - key length= 16	409 - key length= 16	451 - key length= 16	466 - key length= 16
380 - key length= 17	431 - key length= 17	428 - key length= 17	444 - key length= 17	480 - key length= 17

494 - key length= 18	458 - key length= 18	555 - key length= 18	435 - key length= 18	516 - key length= 18
425 - key length= 19	437 - key length= 19	413 - key length= 19	459 - key length= 19	443 - key length= 19
705 - key length= 20	429 - key length= 20	410 - key length= 20	466 - key length= 20	462 - key length= 20

	Методом	Символів	Кронекера	
key= ащпренксб… len= 15	key= рщпленксй… len= 16	key= роплжнксйк… len= 17	key= ьрплжнксйю... len= 18	key= ьрплжнксйю… len= 19
475 - key length= 10	465 - key length= 10	460 - key length= 10	445 - key length= 10	448 - key length= 10
467 - key length= 11	426 - key length= 11	462 - key length= 11	432 - key length= 11	458 - key length= 11
389 - key length= 12	452 - key length= 12	410 - key length= 12	415 - key length= 12	354 - key length= 12
457 - key length= 13	405 - key length= 13	450 - key length= 13	387 - key length= 13	476 - key length= 13
418 - key length= 14	402 - key length= 14	468 - key length= 14	408 - key length= 14	411 - key length= 14
837 - key length= 15	399 - key length= 15	396 - key length= 15	426 - key length= 15	464 - key length= 15
374 - key length= 16	719 - key length= 16	397 - key length= 16	392 - key length= 16	367 - key length= 16
478 - key length= 17	429 - key length= 17	766 - key length= 17	455 - key length= 17	446 - key length= 17
405 - key length= 18	400 - key length= 18	459 - key length= 18	744 - key length= 18	379 - key length= 18
487 - key length= 19	410 - key length= 19	395 - key length= 19	428 - key length= 19	859 - key length= 19
477 - key length= 20	455 - key length= 20	520 - key length= 20	427 - key length= 20	420 - key length= 20

key= ьрплжнос… len= 20
398 - key length= 10
405 - key length= 11
429 - key length= 12
501 - key length= 13
439 - key length= 14
379 - key length= 15
450 - key length= 16
420 - key length= 17
438 - key length= 18
414 - key length= 19
705 - key length= 20

Провівши аналіз результатів бачимо, що за правильно вказаної довжини ключа ми бачимо різке порівняно з іншими зростання, суми символів Кронекера. Також є знову кореляція між кратними числами, але тут вона не зворотня, тобто лише коли менший ключ правильним для кратних більших довжин буде зростання.

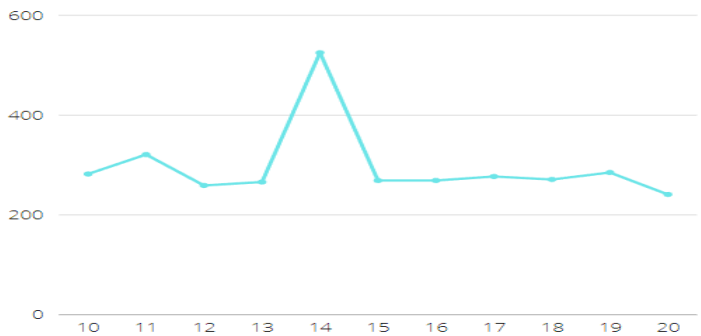
Частина 2.

Наданий шифртекст згідно варіанту потрібно розшифрувати з допомогою знань отриманих в Частині 1.

Пропустимо наш текст через 2 метод та глянемо на результат.

Методом 2
282 - key length= 10
321 - key length= 11
259 - key length= 12
266 - key length= 13
525 - key length= 14
269 - key length= 15
260 - key length= 16
277 - key length= 17
271 - key length= 18
285 - key length= 19
241 - key length= 20

Використавши знання з першого пункту розуміємо , що довжина ключа є 14 тепер залишилось лише підібрати змістовний ключ.



Підбір ключа відбувався так, я провів частотний аналіз, паралельно перевірив на індекс відповідності отримав такі данні ['л', 'п', 'ь', 'ъ', 'о', 'д', 'а', 'ы', 'ц', 'ш', 'в', 'б', 'к', 'ь', 0.056830621393757386]. Я припустив нехай найчастішими літерами ВТ будуть літери «о». Результатом став кдюч «эбомацтникфуьо». Тоді я розшифрував ним текст, але він не мав змісту. Тоді я подумав на, що неправильно розшифрований текст повинен бути схожий і змінював літери серед найчастіших літер ВТ так, щоб отримати бажаний результат. Вкінці я отримав ключ «экомаятникфуко». Після розшифрування цим ключем виявилось, шо текст був уривком з твору «Маятник Фуко» ,автор Умберто Еко.

Надаю уривок:

Итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронно мвеличииописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопе риодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеирраци ональноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаетокру жностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногопол юсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременн ыхмерединственноститочкикрепленияздвойственностиабстрактногоизмерениятроичностич ислаписькрытойчетверичностиквадратногокорнясовершенствакругаещеязналчтонаконцеот весной линииивосстановленнойотточкикрепленияна ходящийсяподмаятникоммагнитныйста билизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечностьдвиженияэтохи траяштукаимеющаяцельюпереборотьсопротивлениематериинокотораянепротиворечитзак онуфуконапротивпомогаетемупроявитьсяпотомучтопомещенныйвпустотулюбойточечный весприложенныйкконцунерастяжимойиневесомойнитиневстречающийнисопротивлениявo зду…..

Висновки:

В цьому практикумі я навчився проводити аналіз тексту зашифрованого шифром Віженера. Я зрозумів що таке індекс відповідності, та як знахдити довжину ключа з допомогою символу Кронекера.